The University of Chicago

THE INTEGERS REPRESENTED BY SETS OF POSITIVE TERNARY QUADRATIC NON-CLASSIC FORMS

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR OF
PHILOSOPHY

DEPARTMENT OF MATHEMATICS
1934

By
OSWALD KARL SAGEN

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS
1936

The University of Chicago

THE INTEGERS REPRESENTED BY SETS OF POSITIVE TERNARY QUADRATIC NON-CLASSIC FORMS

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR OF
PHILOSOPHY

DEPARTMENT OF MATHEMATICS
1934

By
OSWALD KARL SAGEN

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS
1936

R. UNIV.
BIBLIOTHEEK
LEIDEN

TABLE OF CONTENTS

Section		Page
	Introduction	1
1.	Proper representation by sets of forms	2
2.	Classic and non-classic forms	3
3.	Types of non-classic forms	5
4.	A necessary and sufficient condition for proper representation	6
5.	Reduction theorems	8
6.	Necessary and sufficient condition for representation	16
7.	Sufficient conditions for proper representation .	17
8.	Coefficients by type 1	20
9.	Coefficients by type 2	23
10.	Summary	26

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41548406_0139

THE INTEGERS REPRESENTED BY SETS OF POSITIVE TERNARY QUADRATIC NON-CLASSIC FORMS

Introduction. The problem considered in this paper is that of determining all integers represented by a set of positive ternary quadratic non-classic forms having a certain common invariant. This invariant is that integer which is one half of the determinant of twice the given form. A. A. Albert[1] stated and solved the problem for sets of classic forms of a given determinant. The methods employed in this paper are essentially those used by Albert. With slight modifications the following treatment of non-classic ternaries can be made to hold for classic ternaries, the resulting theory being somewhat simpler than that due to Albert. This simplification is by virtue of our Theorem 4. The problem of representation is shown to depend upon that of proper representation. As a result the study reduces essentially to finding, for given integers a and d, conditions for the existence of solutions of the Diophantine equation

$$d + ar^2 + bs^2 = 4abc.$$

The solution of our problem consists in giving explicit formulae for all integers not represented by a set of forms as defined. These formulae depend in part on the maximum power of 4 which divides the invariant defining a given set of forms. In all other respects the formulae are exactly analogous to the expressions obtained by Albert for sets of classic forms.

---

[1] A. A. Albert, "The integers represented by sets of ternary quadratic forms," American Journal of Mathematics, vol. LV, No. 2 (1933), pp. 274-92.

1. Proper representation by sets of forms. We shall first consider any positive ternary quadratic form

$$(1) \qquad f(x, y, z) = ax^2 + by^2 + cz^2 + ryz + szx + txy.$$

We define the integer invariant d of the form (1) by

$$(2) \qquad 2d = \begin{vmatrix} 2a & t & s \\ t & 2b & r \\ s & r & 2c \end{vmatrix} = 2(4abc + rst - ar^2 - bs^2 - ct^2).$$

The determinant (2) is the determinant of the symmetric form $2f(x, y, z)$ and consequently the integer d is an invariant of the form (1) under transformation of determinant unity upon the indeterminates x, y, z. Any form obtained by such transformation applied to (1) is defined as equivalent to $f(x, y, z)$. Any integer A for which there exist integers ξ, η, ζ such that $A = f(\xi, \eta, \zeta)$ is said to be represented by the form $f(x, y, z)$. This representation is proper in case the greatest common divisor of ξ, η, ζ is unity.

The set $\Sigma(d)$ of all forms having the same invariant d is said to represent (properly) an integer A if there exists some form in the set $\Sigma(d)$ by which A is represented (properly).

If a form $f(x, y, z)$ represents A properly, $f(x, y, z)$ is equivalent to a form $f'(x', y', z')$ having A as the coefficient of x'^2.* Thus the proper representation of an integer A by a set $\Sigma(d)$ is equivalent to the existence of some form in the set in which A appears as the coefficient of a square term. Therefore if we set a = A in (1), the problem of showing the existence of

*This statement is proved in Theorem 10, page 12, of Dickson's Studies in the Theory of Numbers for symmetric ternary forms. It also holds for non-symmetric forms since it holds for their doubles which are symmetric.

some form in the set $\sum(d)$ which represents A properly is equivalent to showing the existence of integers b, c, r, s, t which satisfy (2). Moreover, since the forms are to be positive, d, a, b, c, $4ab - t^2$ are all positive. Conversely, if d, a and $4ab - t^2$ are positive the form f is positive and furthermore properly represents the integer a since $f(1, 0, 0) = a$.

For later convenience we shall say that[1] an integer a is a coefficient of $\sum(d)$ if a is properly represented by the set $\sum(d)$.

THEOREM 1. A necessary and sufficient condition that a be a coefficient of $\sum(d)$ is that there exist integers b, c, r, s, t such that

$$d + ar^2 + bs^2 + ct^2 - rst = 4abc, \qquad 4ab - t^2 > 0. \tag{3}$$

2. Classic and non-classic forms. Classic forms are such forms (1) in which the coefficients r, s, t are all even. Non-classic forms are such that at least one of r, s, t is odd. The discussion in Section 1 holds for both classic and non-classic forms. To separate the two kinds of forms we shall need

THEOREM 2. Classic forms are equivalent to classic forms only. Non-classic forms are equivalent to non-classic forms only.

Consider the integral transformation

$$\begin{aligned} x &= u_{11}x' + u_{12}y' + u_{13}z', \\ y &= u_{21}x' + u_{22}y' + u_{23}z', \\ z &= u_{31}x' + u_{32}y' + u_{33}z' \end{aligned} \tag{4}$$

of determinant $|u_{ij}| = 1$. The form $f(x, y, z)$ is carried by this

---

[1] This terminology was introduced by Albert, loc. cit. and he first gave Theorem 1 for sets of classic forms.

transformation into a form

$$(5)\quad f'(x', y', z') = a'x'^2 + b'y'^2 + c'z'^2 + r'y'z' + s'z'x' + t'x'y'$$

with coefficients

$$\begin{aligned}
&a' = f(u_{11},u_{21},u_{31}),\ b' = f(u_{12},u_{22},u_{32}),\ c' = f(u_{13},u_{23},u_{33}),\\
&r' = 2(au_{12}u_{13} + bu_{22}u_{23} + cu_{32}u_{33}) + r(u_{22}u_{33} + u_{32}u_{23})\\
&\qquad + s(u_{13}u_{32} + u_{12}u_{33}) + t(u_{12}u_{23} + u_{22}u_{13}),\\
(6)\quad &s' = 2(au_{11}u_{13} + bu_{21}u_{23} + cu_{31}u_{33}) + r(u_{21}u_{33} + u_{23}u_{31})\\
&\qquad + s(u_{13}u_{31} + u_{33}u_{11}) + t(u_{13}u_{21} + u_{11}u_{23}),\\
&t' = 2(au_{11}u_{12} + bu_{21}u_{22} + cu_{31}u_{32}) + r(u_{21}u_{32} + u_{31}u_{22})\\
&\qquad + s(u_{11}u_{32} + u_{31}u_{12}) + t(u_{11}u_{22} + u_{21}u_{12}).
\end{aligned}$$

Let U_{ij} be the cofactor of the element u_{ij} in the matrix (u_{ij}). Since $|u_{ij}| = 1$ we have

$$\sum_{j=1}^{3} u_{ij}U_{kj} = \begin{cases} 0 \text{ for } k \neq i \\ 1 \text{ for } k = i \end{cases}.$$

Consequently, by (6)

$$\begin{aligned}
r' &\equiv rU_{11} + sU_{21} + tU_{31} \pmod 2,\\
(7)\qquad s' &\equiv rU_{12} + sU_{22} + tU_{32} \pmod 2,\\
t' &\equiv rU_{13} + sU_{23} + tU_{33} \pmod 2,
\end{aligned}$$

and therefore

$$\begin{aligned}
u_{31}r' + u_{32}s' + u_{33}t' &\equiv r\sum_{1}^{3} u_{3j}U_{1j} + s\sum_{1}^{3} u_{3j}U_{2j} + t\sum_{1}^{3} u_{3j}U_{3j} \pmod 2,\\
(8)\qquad &\equiv t \pmod 2.
\end{aligned}$$

By (7) if $r \equiv s \equiv t \equiv 0 \pmod 2$ then $r' \equiv s' \equiv t' \equiv 0 \pmod 2$ and conversely. If one of r, s, t is odd we may without loss assume that t is odd. Then by (8) for t odd we evidently cannot have

$r' \equiv s' \equiv t' \equiv 0 \pmod 2$.

3. Types of non-classic forms. Hereafter we shall consider only forms which are non-classic. These may be divided into two types by the following

DEFINITION. A non-classic form $f(x, y, z)$ is said to be of type X, where X = 1 or 2, if the coefficients r, s, t of f satisfy the congruences

$$(9)\qquad \begin{aligned}(r+1)(s+1)(t+1) &\equiv 0 \pmod 2,\\ (s+1)(t+1) &\equiv X+1 \pmod 2.\end{aligned}$$

The integer a is a coefficient[1] of $\sum(d)$ by type X if there exists some form $f(x, y, z)$ in $\sum(d)$ of type X such that $a = f(1, 0, 0)$.

All transformations by which a form $f(x, y, z)$ is equivalent to a form $f'(x', y', z')$ with $f(1, 0, 0) = f'(1, 0, 0)$ may be obtained from the matrix

$$(10)\qquad T = \begin{pmatrix} 1 & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & u_{32} & u_{33} \end{pmatrix}, \quad u_{22}u_{33} - u_{23}u_{32} = 1.$$

By (6) the coefficients of f' are

$$\begin{aligned} a' &= a,\\ b' &= au_{12}^2 + bu_{22}^2 + cu_{32}^2 + ru_{22}u_{32} + su_{32}u_{12} + tu_{12}u_{22},\\ (11)\quad c' &= au_{13}^2 + bu_{23}^2 + cu_{33}^2 + ru_{23}u_{33} + su_{33}u_{13} + tu_{13}u_{23},\\ r' &= 2(su_{12}u_{13} + bu_{22}u_{23} + cu_{32}u_{33}) + r(u_{22}u_{33} + u_{32}u_{23})\\ &\quad + s(u_{32}u_{13} + u_{12}u_{33}) + t(u_{12}u_{23} + u_{22}u_{13}), \end{aligned}$$

---

[1] Hereafter when we state "a is a coefficient of $\sum(d)$" without specifying type, it is understood that a is a coefficient by at least one type.

$$(11)\qquad \begin{aligned} s' &= 2au_{13} + su_{33} + tu_{23}\,, \\ t' &= 2au_{12} + su_{32} + tu_{22}\,. \end{aligned}$$

Since $u_{33}u_{22} - u_{23}u_{32} = 1$ we have

$$u_{33}u_{22} + u_{23}u_{32} \equiv u_{33}u_{32} + u_{33} + u_{32} \equiv u_{22}u_{23} + u_{23} + u_{22} \equiv 1 \pmod 2.$$

Therefore by (11)

$$\begin{aligned} (s' + 1)(t' + 1) &\equiv (su_{33} + tu_{23} + 1)(su_{32} + tu_{22} + 1) && \pmod 2 \\ &\equiv s(u_{33}u_{32} + u_{33} + u_{32}) + t(u_{22}u_{23} + u_{23} + u_{22}) \\ &\qquad + st(u_{33}u_{22} + u_{23}u_{32}) + 1 && \pmod 2 \\ &\equiv (s + 1)(t + 1) \equiv X + 1 && \pmod 2, \end{aligned}$$

$$\begin{aligned} (r' + 1)(s' + 1)(t' + 1) &\equiv (s + 1)(t + 1)\left[r + 1 + s(u_{32}u_{13} + u_{12}u_{33})\right. \\ &\qquad \left. + t(u_{12}u_{23} + u_{22}u_{13})\right] && \pmod 2 \\ &\equiv (r + 1)(s + 1)(t + 1) \equiv 0 && \pmod 2. \end{aligned}$$

We have proved

THEOREM 3. Any form f' obtained by transformation (10) from a form f of type X is also of type X.

These results enable us to replace a set of integers b, c, r, s, t satisfying (3) and (9) by any set b', c', r', s', t' obtained from (11) so that (3) and (9) hold for the accented letters.

4. A necessary and sufficient condition for proper representation. Suppose that a positive integer a is a coefficient of $\Sigma(d)$ by type X, d positive. By Theorems 1, 3 there exist integers b, c, r, s, t such that

$$(12)\quad d + ar^2 + bs^2 + ct^2 - rst = 4abc, \qquad \Delta = 4bc - r^2 > 0.$$

$$\begin{aligned} (r + 1)(s + 1)(t + 1) &\equiv 0 \pmod 2, \\ (s + 1)(t + 1) &\equiv X + 1 \pmod 2. \end{aligned}$$

The binary quadratic form $\phi(y, z) = by^2 + ryz + cz^2$ has discriminant $-\Delta$ and is positive since $b > 0$. By (12)

$$(13)\quad \phi(s, -t) = bs^2 + ct^2 - rst = 4abc - ar^2 - d = a\Delta - d \quad .$$

Let σ be the g. c. d. of s and t. Then $\sigma + 1 \equiv (s + 1)(t + 1)$ and $\sigma \equiv X \pmod 2$ by (12). Writing $s = \sigma s_1$, $t = \sigma t_1$, $\Psi = \phi(s_1, -t_1)$, we have

$$(14)\quad \phi(s, -t) = \sigma^2 \Psi, \quad f(\sigma, s, -t) = \sigma^2 f(1, s_1, -t_1).$$

Since $\phi(y, z)$ properly represents the positive integer Ψ, there is an equivalent binary $\phi'(y', z')$, of discriminant $-\Delta$, such that

$$\phi'(y', z') = \Psi y'^2 + r'y'z' + c'z'^2.$$

Therefore there exist integers which satisfy

$$(15)\qquad \Delta = 4\Psi c' - r'^2.$$

By (13) $\Psi\sigma^2 = a\Delta - d$ and as a result we have shown by (15) that there exist integers Ψ, c', r', s' such that

$$(16)\qquad ar'^2 + d = \Psi(4ac' - \sigma^2) > 0.$$

By (11) and (12) $r'^2 \equiv r^2 \pmod 4$. By Theorem 1, therefore, equation (16) implies that a is a coefficient of $\sum(d)$ by type X with $(r' + 1)(\sigma + 1) \equiv 0 \pmod 2$ and $\sigma \equiv X \pmod 2$, and for $X = 2$, $a + d \equiv 0 \pmod 4$.

Conversely, if (16) is satisfied as described above, then by Theorem 1 we have for $t = 0$ that a is a coefficient of $\sum(d)$ by type X.

THEOREM 4. *For any positive integers* a *and* d, a *is a coefficient of* $\sum(d)$ *by type* X *if and only if there exist integers* b, c, r, s *such that*

$$d + ar^2 = b(4ac - s^2) > 0,$$

$$(r + 1)(s + 1) \equiv 0 \pmod 2, \qquad s \equiv X \pmod 2,$$

and for $X = 2$, $a + d \equiv 0 \pmod 4$.[1]

5. Reduction theorems. Suppose p is an odd prime not dividing a, and that pa is a coefficient of $\sum(p^2d)$ by type X. By Theorem 4 there exist integers b, c, r, s such that

$$(17) \qquad p^2d + par^2 + bs^2 = 4pabc, \qquad 4bc - r^2 > 0.$$

Therefore $bs^2 \equiv 0 \pmod p$. If $b = b_0p$ then $pd + ar^2 + b_0s^2 = 4ab_0(pc)$. But now if p does not divide b then $s = s_0p$ and $4bc - r^2 = 0 \pmod p$. First let $c = c_0p$, then $pd + ar^2 + (pb)s_0^2 = 4a(pb)c_0$. Now let c be indivisible by p. We select u as a solution of $2bu + r \equiv 0 \pmod p$ and apply to the form in (17) the transformation

$$x = x', \qquad y = y' + uz', \qquad z = z'.$$

By (11) we obtain an equivalent form with coefficients

$$a' = pa, \qquad b' = b, \qquad c' = bu^2 + c + ru,$$

$$r' = 2bu + r, \qquad s' = s, \qquad t' = t = 0.$$

But $4bc' = (2bu + r)^2 + 4bc - r^2 \equiv 0 \pmod p$, and hence $c' \equiv 0 \pmod p$, so again $c' = pc_0'$ and

$$pd + ar^2 + (pb)s_0^2 = 4a(pb)c_0'.$$

Therefore by Theorem 4, a is a coefficient of $\sum(pd)$ by type X.

---

[1] This theorem and its proof hold for sets $\sum(D)$ of classic forms of determinant D. Substituting $d = 4D$, $r = 2R$, $s = 2S$, $t = 2T$, the condition that there exist integers B, C, R, S satisfying $D + aR^2 = B(aC - S^2) > 0$ is necessary and sufficient that a is a coefficient of $\sum(D)$.

Now suppose a is a coefficient of . (pd) by type X. By Theorem 4 there exist integers b, c, r, s : ch that

$$pd + ar^2 + bs^2 = 4abc. \tag{18}$$

If $b = b_0p$ then $p^2d + par^2 + b_0(ps)^2 = 4pab_0($:). If $c = c_0p$ then $p^2d + par^2 + (pb)s^2 = 4pa(pb)c_0$. Now if $bc \not\equiv$ (mod p), let u and v be integers satisfying

$$2au + s \equiv 2bv + r \equiv 0 \quad (\text{mo}(p). \tag{19}$$

Then applying the transformation

$$x = x' + uz', \qquad y = y' + vz', \qquad z = z'$$

to the form in (18) we obtain by (11) an equivalent form with coefficients

$$a' = a, \quad b' = b, \quad c' = au^2 + bv^2 + c + rv + su,$$
$$r' = 2bv + r, \quad s' = 2au + s, \quad t' = t = 0.$$

But $4abc' = b(2au + s^2) + a(2bv + r)^2 + pd$ and by (19) again $c' \equiv 0 \pmod p$ so that

$$p^2d + par'^2 + (pb)s'^2 = 4pa(pb)c_0'.$$

Therefore by Theorem 4, pa is a coefficient of $\sum (p^2d)$ by type X. Hence, a necessary and sufficient condition that pa be a coefficient of $\sum (p^2d)$ by type X is that a is a coefficient of $\sum (pd)$. By induction on p we now have the theorem:

THEOREM 5. Let k be an odd integer without square factor and prime to the integer a. Then ka is a coefficient of $\sum (k^2d)$ by type X if and only if a is a coefficient of $\sum (kd)$ by type X.

Let p be any odd prime not dividing a and let a be a coefficient of $\sum (p^2d)$ by type X. By Theorem 4 there exist

integers b, c, r, s such that

$$p^2d + bs^2 = a(4bc - r^2). \tag{20}$$

We may write $ps_1 = s$. For if s in (20) is not divisible by p we apply the transformation

$$x = x' + uz', \quad y = y', \quad z = z'.$$

By (11) we obtain a set of integers b', c', r', s' satisfying (20) with $s' = 2au + s \equiv 0 \pmod{p}$. Thus we write

$$p^2(d + bs_1^2) = a(4bc - r^2), \quad s = ps_1. \tag{21}$$

If $b = p^2b_2$ then $r = pr_1$ so by (21)

$$d + b_2s^2 = a(4b_2c - r_1^2)$$

and a is a coefficient of $\Sigma(d)$ by type X.

If $b \not\equiv 0 \pmod{p}$ then we may take $c = p^2c_2$ and $r = pr_1$. For let v satisfy $2bv + r \equiv 0 \pmod{p}$ and apply the transformation

$$x = x', \quad y = y' + vz', \quad z = z'.$$

We obtain by (11) a set b', c', r', s' satisfying (21) with

$$b' = b, \quad s' = s, \quad r' = 2bv + r \equiv 0 \pmod{p},$$
$$0 \equiv 4b'c' - r'^2 \equiv 4b'c' \pmod{p^2},$$

and evidently $c' \equiv 0 \pmod{p^2}$. Now by (21)

$$d + bs_1^2 = a(4bc_2 - r_1^2)$$

and a is a coefficient of $\Sigma(d)$ by type X.

There remains the case for $b = pb_1$, $c = pc_1$, $b_1c_1 \not\equiv 0 \pmod{p}$, $r = pr_1$ whence (21) may be written

$$d + pb_1s_1^2 = a(4b_1c_1 - r_1^2). \tag{22}$$

If $d \equiv 0 \pmod p$ or if $(-ad|p) = +1$ we can always select an integer v so that

$$a(2b_1v + r_1)^2 + d = 0 \pmod p. \tag{23}$$

Now applying the transformation

$$x = x', \quad y = y' + vz', \quad z = z', \tag{24}$$

the integers satisfying (22) are replaced by the set

$$\begin{aligned} &b' = b, \quad s' = s, \quad c' = bv^2 + c + r = p(b_1v^2 + c_1 + r_1v), \\ &r' = 2bv + r = p(2b_1v + r_1). \end{aligned} \tag{25}$$

Hence $4ab_1c' = p\left[a(2b_1v + r_1)^2 + a(4b_1c_1 - r_1^2)\right]$

$$\equiv p\left[a(2b_1v + r_1)^2 + d\right] \equiv 0 \pmod{p^2}.$$

Therefore $c' \equiv 0 \pmod{p^2}$ and as above again a is a coefficient of $\sum(d)$ by type X. But (22) also implies

$$pd + b_1s^2 = pa(4b_1c_1 - r_1^2)$$

so that pa is a coefficient of $\sum(pd)$ by type X.

LEMMA. *Let p be an odd prime not dividing a and let a be a coefficient of $\sum(p^2d)$ by type X. If $d \equiv 0 \pmod p$ or $(-ad|p) = +1$ then a is a coefficient of $\sum(d)$ by type X. If $(-ad|p) = -1$ then either a is a coefficient of $\sum(d)$ by type X or pa is a coefficient of $\sum(pd)$ by type X.*

Suppose k is any odd integer. Let a be a coefficient of $\sum(d)$ by type X. By Theorem 4 there exist integers b, c, r, s such that

$$k^2d + a(kr)^2 = (k^2b)(4ac - s^2)$$

and therefore a is a coefficient of $\sum(k^2d)$ by type X. Let ka be a coefficient of $\sum(kd)$ by type X. Then there exist integers b, c, r, s such that

$$k^2d + a(kr)^2 + (kb)s^2 = 4a(kb)(kc)$$

and therefore a is a coefficient of $\sum(k^2d)$ by type X. By repeated application of the lemma and the above results for k we have the following theorem.

THEOREM 6. Let γ be any odd integer relatively prime to ad and let P denote the product of all distinct primes p dividing γ for which $(-ad|p) = -1$. Then a is a coefficient of $\sum(\gamma^2 d)$ by type X if and only if a is a coefficient of $\sum(P^2d)$ by type X. For $P > 1$, a is a coefficient of $\sum(P^2d)$ by type X if and only if either a is a coefficient of $\sum(d)$ by type X or Pa is a coefficient of $\sum(Pd)$ by type X.

Let k be any odd integer and suppose k^2a is a coefficient of $\sum(d)$ by type X. By Theorem 4 there exist integers b, c, r, s satisfying

$$d + a(kr)^2 + bs^2 = 4a(k^2c)b$$

and therefore again by Theorem 4, a is a coefficient of $\sum(d)$ by type X.

THEOREM 7. If k is any odd integer and k^2a is a coefficient of $\sum(d)$ by type X then a is a coefficient of $\sum(d)$ by by type X.

We next obtain results[1] for powers of 4 akin to those obtained for odd integers in the two preceding theorems.

LEMMA 1. For arbitrary integers n, a, d, a is a coefficient of $\sum(4^nd)$ by type 1 if and only if a is a coefficient of

[1]It is here that the principal difference between the classic and non-classic cases arises.

$\sum(d)$ by type 1.

Suppose a is a coefficient of $\sum(4d)$ by type 1. Then by Theorem 4 there exist integers b, c, r, s such that

$$4d + ar^2 = b(4ac - s^2) \qquad (r \text{ even, } s \text{ odd}). \tag{26}$$

We may write $r = 2r_1$, $b = 4b_1$ and hence (26) becomes

$$d + ar_1^2 = b_1(4ac - s^2).$$

Therefore by Theorem 4, a is a coefficient of $\sum(d)$ by type 1. By repeated application of the argument we see that if a is a coefficient of $\sum(4^n d)$ by type 1 then a is a coefficient of $\sum(d)$ by type 1. Conversely, if a is a coefficient of $\sum(d)$ by type 1 there exist by Theorem 4 integers b, c, r, s with s odd such that

$$4^n d + 4^n ar^2 = 4^n b(4ac - s^2) \qquad \text{(for arbitrary n)}.$$

Writing $r_0 = 2^n r$, $b_0 = 4^n b$ we have

$$d + ar_0^2 = b_0(4ac - s^2)$$

and by Theorem 4, a is a coefficient of $\sum(d)$ by type 1.

LEMMA 2. *For arbitrary integers, n, a, d, if $4^n a$ is a coefficient of $\sum(d)$ by type 1 then a is a coefficient of $\sum(d)$ by type 1.*

For, by hypothesis and Theorem 4 there exist integers b, c, r, s with s odd such that

$$d + 4^n ar^2 = b(4 \cdot 4^n ac - s^2).$$

Writing $r_0 = 2^n r$, $c_0 = 4^n c$ we have

$$d + ar_0^2 = b(4ac_0 - s^2)$$

and the lemma follows by Theorem 4. We next prove

LEMMA 3. For arbitrary integers n, a and d, if $4^n a$ is a coefficient of $\sum(4^n d)$ by type 1 then a is a coefficient of $\sum(d)$ by type 1. If $4^n a$ is a coefficient of $\sum(4^n d)$ by type 2 then a is a coefficient[1] of $\sum(d)$. Conversely, if a is a coefficient of $\sum(d)$ by type X then $4^n a$ is a coefficient of $\sum(4^n d)$ by type 2.

Suppose first that $4^n a$ is a coefficient of $\sum(4^n d)$ by type X. By Theorem 4 there exist integers b, c, r, s such that

$$4^n d + 4^n a r^2 = b(4 \cdot 4^n ac - s^2). \tag{27}$$

When X = 1, s is odd and hence $b = 4^n b_0$. Writing $c_0 = 4^n c$, (27) gives

$$d + ar^2 = b_0(4ac_0 - s^2)$$

and by Theorem 4, a is a coefficient of $\sum(d)$ by type 1.

When X = 2, r is odd, $s = 2^m s_0$, s_0 odd, $m > 0$. If $m = n$, (27) becomes

$$d + ar^2 = b(4ac - s_0^2)$$

and a is a coefficient of $\sum(d)$ by type 1. If $m > n$ write $s_1 = 2^{m-n} s_0$ and then (27) becomes

$$d + ar_1^2 = b(4ac - s_1^2)$$

where s_1 is even and hence by Theorem 4, a is a coefficient of $\sum(d)$ by type 2. If $m < n$, (27) implies $b \equiv 0 \pmod{4^{n-m}}$. Writing $b = 4^{n-m} b_0$, $c_0 = 4^{n-m} c$, it follows by (27) that

$$d + ar^2 = b_0(4ac_0 - s_0^2)$$

---

[1] See footnote on page 5.

and hence a is a coefficient of $\sum(d)$ by type 1. Conversely, suppose a is a coefficient of $\sum(d)$ by type X. Then by Theorem 4 there exist integers b, c, r, s with r odd such that

$$d + ar^2 = b(4ac - s^2). \tag{28}$$

Write $s_1 = 2^n s$, then multiplying (28) by 4^n we have

$$4^n d + 4^n a r^2 = b(4 \cdot 4^n ac - s_1^2)$$

and by Theorem 4, $4^n a$ is a coefficient of $\sum(4^n d)$ by type 2 and the proof of Lemma 3 is complete.

Now suppose $a \not\equiv 0 \pmod 4$, $d \not\equiv 0 \pmod 4$. By Lemma 3, $4^h a$ is a coefficient of $\sum(4^h d)$ if and only if a is a coefficient of $\sum(d)$ for h arbitrary. Let h be any integer less than an arbitrary integer g. Then by Lemma 3, $4^h a$ is a coefficient of $\sum(4^g d)$ if and only if a is a coefficient of $\sum(4^{g-h} d)$. But since $4^{g-h} d + a \not\equiv 0 \pmod 4$, a is a coefficient of $\sum(4^{g-h} d)$ by type 1. By Lemma 1 this is equivalent to a being a coefficient of $\sum(d)$ by type 1. Therefore $4^h a$ is a coefficient of $\sum(4^g d)$ if and only if a is a coefficient of $\sum(d)$ by type 1. Now let h be any integer greater than an arbitrary integer g. By Lemma 3 $4^h a$ is a coefficient of $\sum(4^g d)$ if and only if $4^{h-g} a$ is a coefficient of $\sum(d)$. But $4^{h-g} a + d \not\equiv 0 \pmod 4$, so this latter condition is that $4^{h-g} a$ is a coefficient of $\sum(d)$ by type 1. By Lemma 2 this implies that a is a coefficient of $\sum(d)$ by type 1. These results can now be put in the following

THEOREM 8. *Let a and d be any positive integers neither of which is divisible by 4, and let h, g be positive integers. For h = g, $4^h a$ is a coefficient[1] of $\sum(4^g d)$ if and only if a is*

---

[1] See footnote on page 5.

a coefficient of $\sum(d)$. For $h < g$, $4^h a$ is a coefficient of $\sum(4^g d)$ if and only if a is a coefficient of $\sum(d)$ by type 1. For $h > g$, $4^h a$ is a coefficient of $\sum(4^g d)$ implies that a is a coefficient of $\sum(d)$ by type 1.

6. Necessary and sufficient conditions for representation. Let a and d be any positive integers expressed in their unique forms

$$a = L^2M, \qquad d = G^2D, \qquad L = 2^h\lambda, \qquad G = 2^g\gamma$$

where M and D are each without square factor, and where λ, γ are odd. Suppose the set of forms $\sum(d)$ represents a. Then there exists some form $f(x, y, z)$ of determinant d and certain integers ξ, η, ζ such that $a = f(\xi, \eta, \zeta)$. Write

$$\omega = \text{g. c. d.}(\xi, \eta, \zeta), \quad \xi = \omega\xi_1, \quad \eta = \omega\eta_1, \quad \zeta = \omega\zeta_1.$$

Then $a = \omega^2 f(\xi_1, \eta_1, \zeta_1)$ and hence ω divides L. Writing $L = \omega L_1$ we have $L_1^2M = f(\xi_1, \eta_1, \zeta_1)$. Now $f(x, y, z)$ properly represents L_1^2M and thus L_1^2M is a coefficient of $\sum(d)$. By Theorem 7, writing $L_1 = 2^{h_1}\lambda_1$, λ_1 is odd, $h_1 \leqq h$, $4^{h_1}M$ is a coefficient of $\sum(d)$. By Theorem 8 when $h \geqq g$, M is a coefficient of $\sum(\gamma^2 D)$, and when $h < g$ then $h_1 < g$ and M is a coefficient of $\sum(\gamma^2 D)$ by type 1.

Conversely, if M is a coefficient of $\sum(\gamma^2 D)$ by type 1 then by Lemma 1, M is a coefficient of $\sum(G^2D)$ and consequently $\sum(d)$ represents $a = L^2M$. If M is a coefficient of $\sum(\gamma^2 D)$ by type 2 and if $h \geqq g$ then by Theorem 8, $4^g M$ is a coefficient of $\sum(G^2D)$. But then $\sum(d)$ represents $a = 4^h\lambda^2 M$.

THEOREM 9. Express any integers a and d in their unique forms

$$a = L^2M, \qquad d = G^2D, \qquad L = 2^h\lambda, \qquad G = 2^g\gamma,$$

where M and D are each without square factor, λ and γ both odd. Let h and g be any integers. When $h \geqq g$ then the set $\sum(d)$ represents a if and only if M is a coefficient of $\sum(\gamma^2 D)$. When $h < g$ then the set $\sum(d)$ represents a if and only if M is a coefficient of $\sum(\gamma^2 D)$ by type 1.

7. Certain sufficient conditions for proper representation. Throughout the following sections we shall adhere to the notations:

$$\Delta = \gamma^2 D, \quad \gamma \text{ odd}; \qquad D = 2^i \delta, \quad i = 0 \text{ or } 1;$$

$$M = 2^j \mu, \quad j = 0 \text{ or } 1;$$

δ and μ each odd and without square factor.

THEOREM 10. If there exists a factor $q > 1$ which divides δ and is relatively prime to M, then M is a coefficient of $\sum(\Delta)$ by type 1 and also by type 2 whenever $M + \Delta \equiv 0 \pmod 4$.

For the proof write $\delta = q\,\delta_0$ and form the expression

$$p = [Aq]n + [A^{a-1}(w + 1) - 1], \tag{29}$$

where

$$A = 8M\delta_0, \qquad (w|q) = (-1)^{(q+1)/2} \qquad (n \text{ arbitrary}).$$

Since A and q are relatively prime $A^{q-1} \equiv 1 \pmod q$ by Fermat's theorem. By (29)

$$p \equiv w \not\equiv 0 \pmod q, \qquad p \equiv -1 \pmod{A = 8M\delta_0}. \tag{30}$$

Thus the expressions in brackets in (29) are relatively prime. By Dirichlet's theorem[1] on primes in an arithmetic progression, the expression in (29) represents an infinitude of primes. Therefore there is some value of n for which we may take p a prime

[1] P. G. L. Dirichlet, Abhandlungen der Königlichen Akademie der Wissenschaften, Berlin, 1837, pp. 108-110.

integer not dividing some fixed arbitrary integer γ. It immediately follows that we may form the Legendre symbol

$$L_p = (-M\Delta|p) = (-2^{i+j}\mu q\,\delta_o|p). \tag{31}$$

But, $(2|p) = +1$, $(-1|p) = -1$ since $p \equiv -1 \pmod 8$. Also $(\mu|p) = (-1)^{(p-1)(\mu-1)/4}(p|\mu) = +1$ since $p \equiv -1 \pmod{\mu}$, while $(\delta_o|p) = (-1)^{(p-1)(\delta_o-1)/4}(p|\delta_o) = +1$, since $p \equiv -1 \pmod{\delta_o}$, and $(q|p) = (-1)^{(p-1)(q-1)/4}(w|q) = (-1)^{(q-1)/2}(w|q)$, so that $(q|p) = -1$ since $p \equiv w \pmod q$. Therefore $(-M\Delta|p) = +1$. Now define M_o such that $M_oM \equiv 1 \pmod p$. Hence $(-M_o\Delta|p) = +1$ and there exists an odd integer r such that

$$r^2 \equiv -M_o\Delta \pmod p.$$

Therefore

$$\Delta + Mr^2 \equiv 0 \pmod p. \tag{32}$$

Writing $s = 1$, $c = 2\delta_o\left[qn + A^{q-2}(w+1)\right]$ we have $4Mc - s^2 = A\left[qn + A^{q-2}(w+1)\right] - 1 = p$. By Theorem 4 it follows that M is a coefficient of $\Sigma(\Delta)$ by type 1.

If $M + \Delta \equiv 0 \pmod 4$ then by (32)

$$\Delta + Mr^2 = 0 \pmod{4p}. \tag{33}$$

Now setting $s = 2$, $c = 8\delta_o\left[qn + A^{q-2}(w+1)\right]$ we have

$$4Mc - s^2 = 4\left\{8M\,\delta_o\left[qn + A^{q-2}(w+1)\right] - 1\right\} = 4p.$$

Therefore by (31) and Theorem 4, M is a coefficient of $\Sigma(\Delta)$ by type 2 and the proof is complete.

THEOREM 11. *If $\mu = \alpha\delta$ and there exists a factor which is common to γ and α then M is a coefficient of $\Sigma(\Delta)$ by type 1 and also by type 2 whenever $\Delta + M \equiv 0 \pmod 4$.*

For, let $\rho = (\gamma, \alpha) > 1$ and write

$$\gamma = \rho\gamma_1 \ , \quad \alpha = \rho\alpha_1 \ , \quad M_1 = 2^j \alpha_1 \delta \ .$$

Then ρ is prime to $M_1 D$ and is without square factor. By Theorem 10, M_1 is a coefficient of $\sum(\gamma_1^2 \rho D)$ by type 1 and also by type 2 whenever $M_1 + \gamma_1^2 \rho D \equiv 0 \pmod 4$. By Theorem 5, ρM_1 is a coefficient of $\sum(\gamma_1^2 \rho^2 D)$ by type X and the theorem is true.

Suppose γ is prime to α for $\mu = \alpha\delta$. Let

$$\sigma = (\gamma, \delta) \ , \quad \delta = \sigma\delta_1 \ , \quad \gamma = \sigma\gamma_1 \ , D_1 = 2^i \delta_1$$

Evidently σ is without square factor and is prime to $2^j \alpha \delta_1 = M_1$. By Theorem 5, M is a coefficient of $\sum(\Delta)$ by type X if and only if M_1 is a coefficient of $\sum(\sigma\gamma_1^2 D)$ by type X. But $\sigma\gamma_1^2 D = \gamma^2 D_1$. Writing P for the product of all those prime factors p of γ for which $-1 = (-M_1 D_1 | p) = (-2^{i+j}\alpha | p)$, we have by Theorem 6 that M_1 is a coefficient of $\sum(\gamma^2 D_1)$ by type X if and only if either PM_1 is a coefficient of $\sum(PD_1)$ by type X or M_1 is a coefficient of $\sum(D_1)$ by type X.

THEOREM 12. *Suppose* $\mu = \alpha\delta$, α *relatively prime to* γ, $\Delta = \gamma^2 D$, $D = 2^i \delta$, $M = 2^j \mu$,

$$\sigma = (\gamma, \delta) \ , \quad \delta = \sigma\delta_1 \ , \ D = \sigma D_1, \quad M = \sigma M_1,$$

and let $P \geq 1$ *be the product of all distinct factors of* γ *which are primes* p *such that* $(-2^{i+j}\alpha | p) = -1$. *Then* M *is a coefficient of* $\sum(\Delta)$ *by type* X *if and only if either* M_1 *is a coefficient of* $\sum(D_1)$ *by type* X *or* PM_1 *is a coefficient of* $\sum(PD_1)$ *by type* X.

Now in view of Theorems 10, 11, 12 the problem of further proper representations is reduced to the consideration of sets $\sum(D)$ and integers M for which $D = 2^i\delta$, $M = 2^j\alpha\delta$, since PM_1 and PD_1 in the above are evidently each without square factor.

8. Coefficients by type 1.

THEOREM 13. If $D = 2\delta$, $M = \alpha\delta$, then M is a coefficient of $\Sigma(D)$ by type 1.

Form the expression

$$p = [8M]n + [4M - 1] \qquad (n \text{ arbitrary}). \tag{34}$$

By Dirichlet's theorem p is an odd prime by choice of n. Evidently p does not divide MD and we may form the Legendre symbol

$$(-MD|p) = (-2\alpha|p). \tag{35}$$

By (34) $p \equiv 4M - 1 \equiv 3 \pmod 8$ and as a result $(-1|p) = -1$, $(2|p) = -1$. Since $p \equiv -1 \pmod \alpha$ we have $(\alpha|p) = (-1)^{(p-1)(\alpha-1)/4}(-1|\alpha) = +1$. Consequently $(-MD|p) = +1$. Therefore there exists an integer r such that

$$\Delta + Mr^2 \equiv 0 \pmod p. \tag{36}$$

Setting $c = 2n + 1$, $s = 1$, we have

$$4Mc - s^2 = 8Mn + 4M - 1 = p.$$

In view of (36) and Theorem 4 it follows that M is a coefficient of $\Sigma(\Delta)$ by type 1.

In the remainder of this section we shall consider $D = 2^i\delta$, $M = 2^j\alpha\delta$ where $j \geq i \geq 0$.

Suppose that M is a coefficient of $\Sigma(D)$ by type 1. By Theorem 4 there exist integers b, c, r, s with s odd such that

$$2^i\delta + 2^j\alpha\delta r^2 = b(4\cdot 2^j\alpha\delta c - s^2) = bm_0 . \tag{37}$$

Let $q = (s, \delta)$, $s = qs_0$, $\delta = q\delta_0$, then writing $m_0 = qm$ we have $m = 4\cdot 2^j\alpha\delta_0 c - qs_0^2$. Evidently m is prime to δ and hence by (37)

(38) $$2^i + 2^j \alpha r^2 \equiv 0 \pmod{m}.$$

Since m is odd, and if $m > 1$, the Jacobi symbol

(39) $$J_m = (-2^{i+j}\alpha \,|\, m) = +1.$$

Evaluating we find

(40) $$J_m = (-1|m)(2|m)^{i+j}(\alpha|m) = (-1)^e(-\alpha|q)$$

where

$$8e \equiv 4(m-1) + (i+j)(m^2-1) + 2(\alpha-1)(m-1) + 4(\alpha-1) + 2(\alpha-1)(q-1) + 4(q-1) \pmod{16}.$$

But since $m \equiv -q \pmod{4\cdot 2^j}$, $j \geq i \geq 0$, we have

$$(i+j)m^2 \equiv (i+j)[8\cdot 2^j c + q^2] \equiv (i+j)q^2 \pmod{16}.$$

Consequently,

(41) $$8e \equiv 8 + (i+j)(q^2-1) \pmod{16}.$$

Writing $A = 2^{j-i}\alpha$, $D_0 = 2^i \mathcal{S}_0$, $M_0 = 2^j \alpha \mathcal{S}_0$, we have by (39), (40), (41),

(42) $$-1 = (-2^{i+j}\alpha|q) = (-2^{j-i}\alpha|q) = (-A|q).$$

Now suppose $m = 1$. Then $4\cdot 2^j \alpha \mathcal{S}_0 c = qs_0^2 + 1$ and hence $q + 1 \equiv 0 \pmod{4\cdot 2^j}$. But $(qs_0)^2 \equiv -q \pmod{\alpha}$ and therefore the Jacobi symbol $(-q|\alpha) = +1$ and as a result

$$(\alpha|q) = (-1)^{(\alpha-1)(q-1)/4 + (q-1)/2} = (-1)^{(q+1)(\alpha-1)/4} = +1.$$

Therefore again $(-2^{i+j}\alpha|q) = (-\alpha|q) = -1$. If $q = 1$, then by (40) $J_m = -1$, a contradiction. Thus (42) must hold for some factor $q > 1$.

Conversely, suppose there exists a factor $q > 1$ which satisfies (42). Form the expression

$$p = [8\cdot 2^j \alpha \mathcal{J}_0]n - [q] \qquad \text{(n arbitrary).} \tag{43}$$

The expressions in brackets are relatively prime so by Dirichlet's theorem p is an odd prime for some value of n. Since p does not divide a we form the Legendre symbol

$$(-M_0D_0|p) = (-2^{i+j}\alpha|p) = (-1)^u(-\alpha|q) \tag{44}$$

where

$$\begin{aligned} 8u &\equiv 4(p-1) + (i+j)(p^2-1) + 2(\alpha-1)(p-1) + 4(\alpha-1) \\ &\quad + 2(\alpha-1)(q-1) + 4(q-1) \pmod{16} \\ &\equiv 4(q+1) + (i+j)(q^2-1) \\ &\quad + 2(\alpha-1)[(q+1) + 2 + (q-1)] + 4(q-1) \pmod{16} \\ &\equiv 8 + (i+j)(q^2-1) \pmod{16}. \end{aligned}$$

Thus $(-M_0D_0|p) = -(-2^{i+j}\alpha|q) = +1$. Therefore there exists an odd integer r such that

$$\begin{aligned} D_0 + M_0r^2 &\equiv 0 \pmod{p}, \\ D + Mr^2 &\equiv 0 \pmod{qp}. \end{aligned} \tag{45}$$

Let $c = 2n$, $s = q$, then (43) implies

$$4Mc - s^2 = 8M_0qn - q^2 = qp$$

and by (45) and Theorem 4 it follows that M is a coefficient of $\Sigma(D)$ by type 1.

THEOREM 14. *Let $M = AD$ be without square factor. M is a coefficient of $\Sigma(D)$ by type 1 if and only if there exists an odd integer $q > 1$ such that q divides D and $(-A|q) = (-2^{i+j}\alpha|q) = -1$.*

9. Coefficients by type 2. We again consider integers M and sets $\Sigma(D)$ with $M = 2^j \alpha\delta$, $D = 2^i\delta$, $\alpha\delta$ odd and without square factor, i, j = 0 or 1. A necessary condition that M be a coefficient of $\Sigma(D)$ by type 2 is that $M + D \equiv 0 \pmod 4$. This evidently requires that $i \neq j$, and that for $i = j = 0$ we have $\alpha \equiv 3 \pmod 4$.

THEOREM 15. If M is a coefficient of $\Sigma(D)$ by type 2 then $M \equiv D \pmod 2$. Let $M = 2\alpha\delta$, $D = 2\delta$. If $\alpha \equiv 3 \pmod 8$ then M is a coefficient of $\Sigma(D)$ by type 2. If there exists some factor $q > 1$ of such that $(-\alpha|q) = +1$ and if $\alpha \equiv 1 \pmod 4$ then M is a coefficient of $\Sigma(D)$ by type 2.

When $\alpha \equiv 3 \pmod 8$ we form the expression

$$(46)\quad p = \alpha\delta(2n + 1) - 2 = [2\alpha\delta]n + [\alpha\delta - 2], \text{ (n arbitrary).}$$

By Dirichlet's theorem we choose n so that p is an odd prime. We form the Legendre symbol

$$(47)\quad \begin{aligned}(-\alpha|p) &= (-1)^{(p-1)/2 + (p-1)(\alpha-1)/4}(-2|\alpha) \\ &= (-1)^{(\alpha-1)/2 + (\alpha^2-1)/8} = +1.\end{aligned}$$

Therefore there exists an odd integer r such that

$$1 + \alpha r^2 \equiv 0 \pmod p.$$

Hence

$$(48)\quad 2\delta + 2\alpha\delta r^2 \equiv 0 \pmod{8p}.$$

Setting $c = 2n + 1$, $s = 4$, we have by (46)

$$4Mc - s^2 = 4[M(2n + 1) - 4] = 8p .$$

From (48) and Theorem 4 it follows that M is a coefficient of $\Sigma(\Delta)$ by type 2.

When $\alpha \equiv 1 \pmod 4$ and $\delta = q\delta_1$ with $(-\alpha|q) = +1$, we form the expression

$$(49)\quad p = 2\alpha\delta_1(2n+1) - q = [4\alpha\delta_1]n + [2\alpha\delta_1 - q] \quad (n \text{ arbitrary}).$$

The expressions in brackets are evidently relatively prime to each other. By Dirichlet's theorem p can then be fixed so that p is an odd prime. Hence we may form the Legendre symbol

$$(50)\qquad (-\alpha|p) = (-1)^u(\alpha|q) = (-1)^{u+(q-1)/2},$$

where

$$4u \equiv 2(p-1) + (p-1)(\alpha-1) + 2(\alpha-1)(q-1) \pmod 8$$
$$\equiv 2(2-q-1) \pmod 8.$$

Evidently $(-\alpha|p) = +1$ and therefore there exists an odd integer r such that

$$1 + \alpha r^2 \equiv 0 \pmod p.$$

Hence

$$(51)\qquad 2\delta + 2\alpha\delta r^2 \equiv 0 \pmod{4qp}.$$

Writing $c = 2n+1$, $s = 2q$, we have by (49)

$$4Mc - s^2 = 8\alpha\delta(2n+1) - 4q^2 = 4qp.$$

Therefore by (51) and Theorem 4, M is a coefficient of $\sum(D)$ by type 2. We now prove the final necessity condition.

THEOREM 16. *Let* $D = 2^i\delta$, $M = 2^i\alpha\delta$, *and let* M *be a coefficient of* $\sum(D)$ *by type* 2. *If* $i = 0$ *then* $\alpha \equiv 3 \pmod 4$ *and there exists a factor* $q > 1$ *of* δ *such that* $(-\alpha|q) = -1$. *If* $i = 1$ *and* $\alpha \equiv 7 \pmod 8$ *then there exists a factor* $q > 1$ *of* δ *such that* $(-\alpha|q) = -1$.

Since M is a coefficient of $\sum(D)$ by type 2, $M + D \equiv 0 \pmod 4$. Hence for $i = 0$, $\alpha \equiv 3 \pmod 4$. By Theorem 4 there exist integers b, c, r, s with r odd and s even such that

$$2^i \delta + 2^i \alpha \delta r^2 = b(4 \cdot 2^i \alpha \delta c - s^2) = 4bm_0, \tag{52}$$

$$m_0 = Mc - s_0^2, \qquad s = 2s_0.$$

Let $q = (\delta, m_0)$, $\delta = q\delta_0$, $m_0 = qm$, $s_0 = qs_1$

$$m = 2^i \alpha \delta_0 c - qs_1^2. \tag{53}$$

Evidently q is prime to δ_0 since δ was without square factor, and m is prime to δ_0. Write m in its unique form $m = 2^e v$ where v is odd. Suppose first that $v > 1$. By (52) $1 + \alpha r^2 \equiv 0 \pmod v$. Therefore the Jacobi symbol

$$(-\alpha|v) = (-1)^{(v-1)/2 + (v-1)(\alpha-1)/4}(v|\alpha) = +1. \tag{54}$$

Since $m \equiv -qs_1^2 \pmod \alpha$

$$(-q|\alpha) = (m|\alpha) = (2|\alpha)^e(v|\alpha)$$

and hence (54) implies

$$(\alpha|q) = (-1)^u(2|\alpha)^e \tag{55}$$

$$4u \equiv 2(v-1) + (v-1)(\alpha-1) + (\alpha-1)(q-1) + 2(\alpha-1) \pmod 8$$

$$\equiv 2(q+1) \pmod 8.$$

For $\alpha \equiv 7 \pmod 8$, $(2|\alpha) = +1$. For $i = 0$, $\alpha \equiv 3 \pmod 8$, we have by (52), $4bm_0 = \delta(1 + \alpha r^2) \equiv 4 \pmod 8$, so that m_0 and hence m is odd. Therefore $e = 0$ and $(2|\alpha)^e = +1$. Consequently the condition (55) reduces to

$$(-\alpha|q) = -1. \tag{56}$$

Lastly let $v = 1$. Then by (53) $- qs_1^2 = 2^e \pmod{\alpha}$ and the Jacobi symbol $(- 2^e q | \alpha) = + 1$. This last implies

$$(- \alpha | q) = (-1)^{(\alpha-1)/2 + (\alpha-1)(q-1)/4} (2|\alpha)^e.$$

Since $\alpha \equiv 3 \pmod 4$, we have again

$$(- \alpha | q) = (-1)^{(q+1)/2 + (q-1)/2} (q|\alpha)^e = - 1$$

which completes the proof.

In Theorems 15 and 16 we note that

$$(- M_0 D_0 | q) = (- \alpha | q)$$

where

$$\delta = q \delta_0, \quad D_0 = 2^i \delta_0, \quad M_0 = AD_0, \quad M = AD.$$

10. Summary. Let $D = 2^i \delta$, $\Delta = \gamma^2 D$, $M = 2^j \mu$ be any integers such that $\gamma \delta \mu$ is odd, δ and μ are each without square factor and i, j take the values 0 or 1 only. By Theorems 10 and 11, M is a coefficient of $\Sigma(\Delta)$ by type 1 except possibly when $\mu = \alpha \delta$, $(\gamma, \alpha) = 1$. For such integers Theorems 13 and 12 imply M is a coefficient of $\Sigma(\Delta)$ by type 1 except possibly when $j \geqq i$, or in other words when $M = AD$. By Theorems 14 and 12, M is a coefficient of $\Sigma(\Delta)$ by type 1 for $M = AD$ if there exists some prime p which divides γ and is such that $(- A|p) = - 1$. As a result by Theorems 14 and 12, M is a coefficient of $\Sigma(\Delta)$ by type 1 if a nd only if M is not of the form $M = AD$ where $(- A|p) = + 1$ for every odd prime p dividing Δ.

It remains to examine whether M is a coefficient of $\Sigma(\Delta)$ by type 2 when not by type 1. In this case we find by Theorems 15, 16 and 12 that M is a coefficient of $\Sigma(\Delta)$ by type 2 for $M \equiv D \equiv 0 \pmod 2$ if and only if $A \not\equiv 7 \pmod 8$. Theorems 15, 16 and 12 imply that M is not a coefficient of $\Sigma(\Delta)$ by type 2 for

$M \equiv D \equiv 1 \pmod 2$ and for $M \equiv D \pmod 2$.

Now upon applying Theorem 9 we obtain the final result

THEOREM 17. *Express any positive integers* a *and* d *in their unique forms*

$$a = 4^h \lambda^2 M, \qquad d = 4^g \gamma^2 D,$$

where $\lambda\gamma$ *is odd,* M *and* D *are each without square factor. If* $h \geq g$, *the set* $\sum(d)$ *represents all integers* a *except those for which*

$$M = AD, \qquad A \equiv 7 \pmod 8,$$

$(-A|p) = +1$ *for every prime* p *dividing* d. *If* $h < g$, *the set* $\sum(d)$ *represents all integers* a *except those for which*

$$M = AD,$$

$(-A|p) = +1$ *for every odd prime* p *dividing* d.

COROLLARY. *Every set* $\sum(d)$ *represents no integer of the form*

$$4^g D(8nd - 1)$$

and hence no $\sum(d)$ *represents all positive integers.*

This last result proves the well-known fact that no positive ternary quadratic non-classic form represents all positive integers.

VITA

Oswald Karl Sagen was born March 27, 1906 in La Crosse, Wisconsin. He attended the public schools of that city and graduated from high school in 1922. He entered Luther College, Decorah, Iowa and was granted the A. B. degree in 1926. After one term as a graduate student at the University of Iowa he became a graduate assistant in mathematics at the University of Pittsburgh and held this appointment for two and a half years until February, 1929. At that time he returned to Luther College as an instructor and taught there until June, 1931. He matriculated at the University of Chicago in the summer quarter of 1928. He was in attendance at Chicago for eleven quarters during the years 1928-1934.

At Pittsburgh he studied under Professors Foraker, Swartzel and Taylor of the mathematics department. At Chicago he attended courses given by Professors Albert, Barnard, Bartky, Blaschke, Bliss, Bompiani, Dickson, Graves, Lane, Logsdon, Lunn, MacDuffee, MacMillan and Murnaghan. He wishes to acknowledge his deep appreciation of their guidance and especially his indebtedness to Professor Albert under whose direction this thesis was prepared.